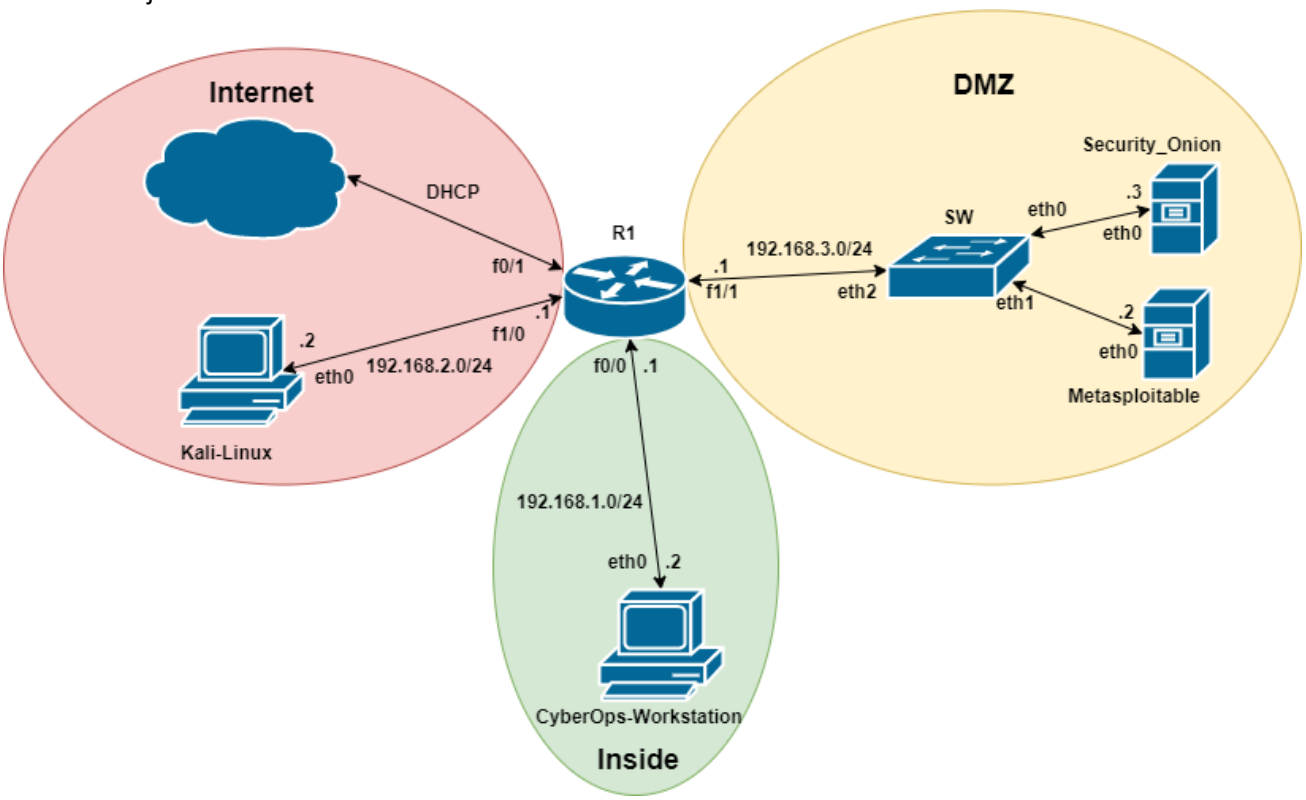
RBI / Cvičenie 01 / Základná konfigurácia a práca so zariadeniami

Topológia

Upozornenie: Názvy rozhraní nemusia sedieť s názvami v GNS3 topológii, preto prosíme prvého študenta, ktorý si zobrazí rozhrania a doplní popisky v topológii, aby poslal screen shot obrázku do teamsu, a následne ho aktualizujeme.



Požiadavky

- Internetové pripojenie
- Pripojenie na školskú VPN (ak sme mimo laboratórií na UNIZA)
- GNS3 vo verzii 2.2.29
- Odporúčame aplikáciu MobaXterm na pripojenie k zariadeniam (rýchlejšie pripojenie ako v GNS3)

Scenár a inštrukcie

Toto laboratórne cvičenie vzniklo na základe týchto oficiálnych Netacad labov a ich doplnením:

- 4.2.6 - Working with Text Files in the CLI
- 4.2.7 - Getting Familiar with the Linux Shell
- 4.3.4 - Linux Servers

Cvičenie je zamerané na prípravu virtuálnej infraštruktúry, na ktorej sa bude pracovať na ďalších cvičeniach:

Názov VM	Názov súboru	Veľkosť Ova súboru	Minimum RAM	Názov súboru v GNS3
CyberOps Workstation VM	cyberops_workstation.ova	3,51 GB	1 GB	cyberops_workstation-disk001.vdi
Security Onion VM	security_onion.ova	2,86 GB	4 GB	Security_Onion_3G-disk001.vdi
Metasploitable	Metaspoitable.vmdk		1 GB	Metasploitable_[20170720]-disk001.vdi
Router				c7200-adventerprisek9-mz.155-2.XB.bin
Switch				vios_l2-adventerprisek9-m.vmdk.SSA.152-4.0.55.E
Kali			2 GB	Kali-linux-2022.vdi

Pracovať možno s danými VMs v týchto prostrediach:

A. na GNS3 servery
   a. remote, na našom KIS servery (IP adresy servera oznámi vyučujúci na cvičení)
      i. Výhody: menšia záťaž na úvodný rozbeh, nezaťažujete zdroje svojho PC
      ii. Nevýhody: pri väčšom vyťažení servera, na ktorom pracujú aj iní študenti, môže byť server pomalšie responzívnejší
   b. local, na GNS3 lokálne u seba na svojom PC (tento variant odporúčame)
      i. Výhody: máte správu nad svojím projektom v GNS3, nikto vám ho nezmaže, s nikým sa nedelíte o zdroje svojho PC, na ktorom pracujete
      ii. Nevýhody: potrebné mať PC s dostatočným výkonom, a venovať čas rozbehnutiu projektu s VMs v GNS3
   c. Pre oba varianty – pokračujete ďalej postupom ktorý nájdete nižšie „**Príprava pre variant A: Topológia v GNS3**“
B. vo VirtualBoxe
   a. na školskom PC – bude možné až od 2. až 3. týždňa semestra v škol roku 2022/23, a iba na 10 PCs v RB003
      i. Výhody: VMs máte pripravené
      ii. Nevýhody: nie je možné prístup k VMs v labe zabezpečiť, takže iný študenti vám môžu úmyselne, alebo neúmyselne VMs zmazať/zmeniť
      iii. Pri tomto variante pokračujete na cvičení postupom, ktorý nájdete nižšie “**Práca so zariadeniami**”
   b. na svojom osobnom PC/notebooku
      i. Výhody: bezpečnosť, za všetko si ručíte sami, niečo sa naučíte aj pri príprave prostredia a VMs
      ii. Nevýhody: budete mať zjednodušenú topológiu (ďalej od reality), obsahujúcu iba 4 koncové zariadenia, čiže bez smerovača a prepínača, všetky VMs budú v jednej sieti (všetky úlohy v laboch sa ale budú ďat zrealizovať); potrebujete dostatočné zdroje na svojom PC pre rozbeh 4 VMs
      iii. Pre tento variant pokračujete ďalej postupom, ktorý nájdete nižšie „**Príprava pre variant B: Nasadenie vo VirtulBoxe**“

C. v NDG online labe
   a. Výhody: všetko máte pripravené ako na podnose, vyladený výkon, pripravené VMs v online topológii
   b. Nevýhody: služba je platená – 40 dolárov na 6 mesiacov; je potrebné mať vždy pripojenie na internet, pre prístup k labu
   c. Pre tento variant máte info v 1. prednáške, je potrebné si vyriešiť prístup k labu v prípade záujmu do 1. cvičenia. Ďalej budete pokračovať na cvičení postupom, ktorý nájdete nižšie "**Práca so zariadeniami**"

Ak chcete pracovať so zariadeniami vo VirtualBoxe, nie v GNS3, tak si vyberiete, či budete pracovať na svojich počítačoch alebo na školských. Ak pracujete na svojich počítačoch, tak sa odporúča aby ste si nainštalovali VirtualBox a taktiež virtuálne zariadenia do VirtualBox-u pred samotným cvičením. Pri práci na školských počítačoch sú už všetky potrebné náležitosti nainštalované a pripravené (dostupné až od 2. až 3. týždňa semestra v škol. roku 2022/23), takže môžete prejsť na časť „**Práca so zariadeniami**".

Začína sa **konfiguráciou IP adries** na zariadeniach v pripravenej topológii v GNS3 na školskom serveri alebo na lokálnom serveri. Na školský server sa pripojíme pomocou VPN, ak sa nachádzame mimo počítačového laboratória na KIS (návod tu). V topológii budeme realizovať konfiguráciu IP adries na všetkých podľa nižšie uvedeného adresného plánu. Študenti budú rozdelení po dvoch do skupín a v rámci skupiny si rozdelia zariadenia, ktoré nakonfigurujú. Ak pracujete na lokálnom GNS3 serveri, tak pracujete samostatne. Na záver je dôležité overenie konfigurácie.

V ďalšej časti sa pozrieme na **prácu so zariadeniami pomocou príkazov v terminály Linuxu**. Ak tieto príkazy ešte nepoznáte z iných predmetov, tak na poslednej strane je návod k jednotlivým príkazom, ktoré v tomto cvičení budeme používať a ktoré budeme používať aj v nasledujúcich cvičeniach.

Adresný plán (platí pre GNS3 topológiu)

Zariadenie	Rozhranie	IP Adresa	Maska podsiete	Default Gateway
R1	f0/0	192.168.1.1	255.255.255.0	N/A
	f0/1	DHCP		
	f1/0	192.168.2.1	255.255.255.0	N/A
	f1/1	192.168.3.1	255.255.255.0	N/A
CyberOps-Workstation	eth0	192.168.1.2	255.255.255.0	192.168.1.1
Kali-Linux	eth0	192.168.2.2	255.255.255.0	192.168.2.1
Metasploitable	eth0	192.168.3.2	255.255.255.0	192.168.3.1
Security_Onion	eth0	192.168.3.3	255.255.255.0	192.168.3.1

Používatelia

Názov	Meno	Heslo
Kali Linux	kali	kali
Metasploitable	msfadmin	msfadmin
Security Onion	analyst	cyberops
CyberOps Workstation	analyst	cyberops

Príprava pre variant A: Topológia v GNS3

V prípade práce na svojich PC odporúčame, aby ste si nástroj GNS3 stiahli a nainštalovali pred cvičením – t.j. zrealizujte krok 0 z postupu nižšie (Inštalácia GNS3 klienta).

Poznámka: Všetky články k tomuto nástroju, jeho nasadeniu a riešeniu problémov, ktoré boli spísané na KIS sú uverejnené na:

- https://nil.uniza.sk/sk/category/network_simulation_and_modelling/gns3/
- https://nil.uniza.sk/category/network-simulation-modelling/network-simulation-modelling-gns3/

Dôležité je upozorniť, že články sú v angličtine, ale aj slovenčine a niektoré sú len v jednom jazyku, preto je užitočné prepnutie jazykov v pravom hornom rohu a hľadať články v oboch jazykoch.

0. **Inštalácia GNS3 klienta (vykonávate len ak pracujete na svojich PC)**
    a. Práca na školskom serveri: https://nil.uniza.sk/sk/navod-na-instalaciu-gns3-klienta/
        i. **Poznámka:** Pre pripojenie sa na školský GNS3 server, je potrebné mať GNS3 klienta vo verzii 2.2.29, ktorý je dostupný na stiahnutie tu: *https://github.com/GNS3/gns3-gui/releases/download/v2.2.29/GNS3-2.2.29-all-in-one.exe*
        ii. **Poznámka:** IP adresa pre katedrový GNS3 server je 158.193.152.64
    b. **Práca na lokálnom serveri:**
        i. Stiahneme si topológiu z Teams-u. Prejdeme do kanálu predmetu > General > Files a stiahneme *RBI-topology-2022-TEMPLATE.gns3project* (11GB).
        ii. V tom istom priečinku na Teams-e si otvoríme dokument *navod_na_instalaciu_GNS3_ako_klient-localServer.docx* a postupujeme ďalej podľa neho
        iii. Pripojíme náš lokálny GNS3 server na internet (zatiaľ nekonfigurujeme nič, len opravíme prepojenie/linku)
            1. Po úspešnom importe otvoríme projekt cez „File“->“Open project“ a zvolíme priečinok pre náš importovaný projekt v ktorom zvolíme .gns3 súbor a klikneme na „Otvoriť“
            2. Vymažeme linku medzi smerovačom a internetom, a taktiež vymažeme oblak pre internet
            3. V ľavej lište klikneme na „Browse End Devices“ a zvolíme „Cloud“, ktorý prenesieme do našej topológie. V okne, ktoré sa zobrazí, vyberieme „GNS3 VM“ ako server a klikneme na „OK“.
            4. Pridáme nový link z routra na náš novo pridaný „Cloud“. V ľavej lište klikneme na „Add a link“, klikneme na router a vyberieme interface „FastEthernet0/1“ a následne klikneme na „Cloud“ a vyberieme rozhranie „eth1“

1. **Otvoríme projekt s pripravenou topológiou**
    a. Spustíme si GNS3
        i. Hore vpravo zvolíme File>Open project>Projects Library
        ii. Nájdeme projekt s názvom *RBI-topology-2022-TEMPLATE*
            1. Klikneme naň a stlačíme tlačidlo Duplicate
            2. Zvolíme názov RBI-topology-2022-skupina-XY
                a. Za XY doplníme skupinu a za YYYY doplníme rok
            3. Stlačíme tlačidlo OK a počkáme, kým sa vytvorí projekt

Upozornenie: Ak v hlavnom okne nevidíte topológiu, choďte do „View“ a kliknite na „Fit in view“.

2. **Konfigurácia zariadení**
    a. V rámci skupiny si rozdelíme zariadenia (ak pracujete na školskom serveri)
        i. Zariadenia musia byť spustené (Zelené tlačidlo pri zariadení hore vpravo v Topology Summary)
            1. Zariadenie spustíme, keď klikneme na zariadenie PTM a vyberieme Start
                a. Môžeme spustiť aj celú topológiu hore v hlavnom paneli veľké zelené tlačidlo Start/Resume all nodes
                b. Ak by sa zariadenie nespustilo odporúčame s ním trocha pohýbať
    b. Pripojíme sa na jednotlivé zariadenia
        i. Odporúčame použiť nástroj MobaXterm (alternatíva putty)
            1. Stiahneme tu a nainštalujeme
            2. Po spustení otvoríme v hornej lište záložku Session
            3. Vyberieme pripojenie podľa zariadenia
                a. Väčšina je VNC, ale treba pozrieť v Topology Summary v GNS3
            4. Zadáme IP adresu pripojenia a port
                a. Nájdeme v Topology Summary
                b. Odporúčame si v záložke Bookmark settings uložiť pripojenie, pretože ho budeme potrebovať aj v nasledujúcich cvičeniach
                    i. IP adresa ostáva nezmenná, ale menia sa porty, preto pri duplikácii cvičenia treba zmeniť, prípadne si vytvárať pripojenia k jednotlivým cvičeniam zvlášť
        ii. Môžeme sa pripojiť aj pomocou GNS3
            1. Klikneme pravým na zariadenie a vyberieme console
                a. Ak sa nepôjde pripojiť ani po dlhšej chvíli, resetovať zariadenie poprípade ho vymazať a znova vložiť do topológie
    c. Nakonfigurujeme postupne zariadenia
        i. Zvolíme meno a heslo podľa uvedenej tabuľky vyššie
        ii. Otvoríme si terminál
            1. Zadáme príkaz pre priradenia IP adresy v Linux (pomôcka v tabuľke).

            Upozornenie: Ak by vám náhodou nešli zadávať čísla do niektorého z terminálov príslušného zariadenia, treba ísť do „Applications->Settings->Keyboard“ a v záložke „Layout“ si vybrať napríklad slovenskú klávesnicu a odstrániť pôvodnú.

            2. Pridáme default gateway
            3. Pri opätovnom spúšťaní všetkých zariadení, okrem smerovača, prepínača a CyberOps-Workstation, sa ich sieťová konfigurácia načítava zo súboru „/etc/network/interfaces“, preto je potrebné dané sieťové nastavenia zaviesť aj do tohto súboru
                a. Otvoríme si súbor „/etc/network/interfaces“ ako root v editore **nano**, alebo v akokoľvek inom textovom editore
                b. Ak v súbore existuje sekcia s názvom „The primary network interface“, tak ju upravíme, ak nie tak ju najskôr vytvoríme a potom do nej dopíšeme príkazy
                c. Príklad, ako má vyzerať súbor s danou sekciou a jej príkazmy pre zariadenie **Kali Linux**, môžeme vidieť na obrázku nižšie

```
# The primary network interface
auto eth0
###iface eth0 inet dhcp
allow-hotplug eth0
iface eth0 inet static
address 192.168.2.2
netmask 255.255.255.0
gateway 192.168.2.1
```

d. Niektoré príkazy v sekcií „The primary network interface“ majú aj argument:

   i. *address <ip adresa pre zariadenie>*
   ii. *netmask <maska podsiete pre zariadenie>*
   iii. *gateway <ip adresa pre gateway>*

e. Takto upravený súbor môžeme uložiť a zavrieť. Ak máme súbor otvorený v textovom editore **nano,** tak pomocou kláves **ctrl+x** ho zavrieme, kde ale následne budeme vyzvaný, či chceme súbor uložiť alebo nie, pre uloženie zadáme „y“ a následne budeme vyzvaný, či chceme zápis vykonať do rovnakého súboru, stlačíme enter, pretože chceme

f. Pre zariadenie CyberOps-Workstation, upravujeme súbor „etc/systemd/network/25-wired.network“, kde si ho otvoríme takým istým spôsobom a jeho obsah zmeníme podľa obrázka nižšie a súbor uložíme

```
 GNU nano 4.9.2                    25-wired.network
[Match]
Name=eth0

[Network]
#DHCP=ipv4
Address=192.168.1.2/24
Gateway=192.168.1.1
DNS=192.168.1.1
```

4. Nastavíme IP adresy aj pre rozhrania smerovača.
5. Overíme našu konfiguráciu výpisom priradených IP adries na zariadení
   a. IP adresy volíme podľa adresného plánu
   b. Overíme, pripojenie k ostatným zariadeniam pomocou príkazu ping

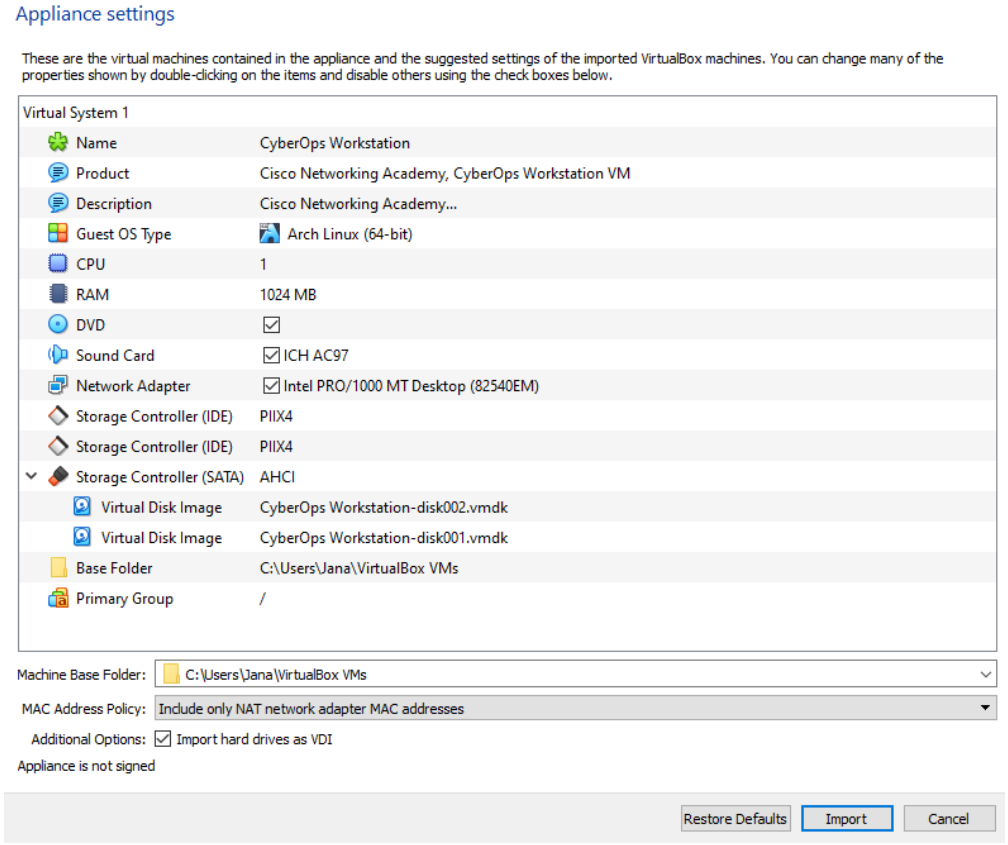
d. Pripojenie na internet
   i. Na R1 nastavíme dhcp
      1. Príkaz *int <fx/x>*
         a. ip address dhcp
   ii. Nezabudnite nakonfigurovať preklad adries (pat)
   iii. Otestujte konektivitu medzi každými 2 zariadeniami, aj z každého zariadenia do inernetu

Príprava pre variant B: Nasadenie vo VirtualBox-e

Nasadenie podľa krokov nižšie je časovo náročné, preto odporúčame aby ste to zrealizovali v predstihu, pred cvičením.

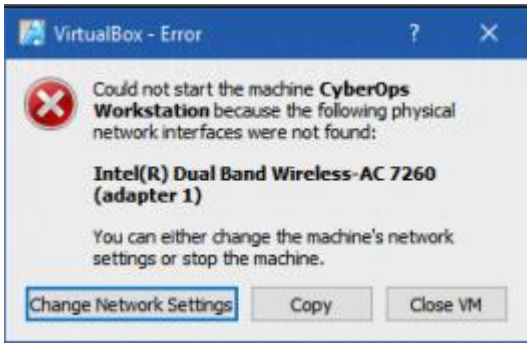
CyberOps Workstation VM a Security Onion VM

1. Stiahneme a nainštalujeme VirtualBox
   a. Prejdeme na stránku http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html
      i. Vyberieme si správny inštalačný súbor pre svoj operačný systém.
      ii. Po stiahnutí inštalačného súboru pre VirtualBox, spustíme inštaláciu a prijmeme predvolené nastavenia.
2. Stiahneme a importujeme image súbory pre virtuálne zariadenia
   a. Prejdeme na stránku https://netacad.com/portal/content/cyberops-associate-virtual-machines-vms (najskôr je potrebné sa prihlásiť do netacad-u)
      i. Stiahneme cyberops_workstation.ova a security_onion.ova image súbor.
   b. Importujeme virtuálne zariadenia do VirtualBox-u
      i. Otvoríme VirtualBox a zvolíme **File > Import Appliance...** pre importovanie image-u virtuálneho zariadenia.
      ii. V **Appliance to import** okne, špecifikujeme miesto .OVA súboru (cyberops_workstation.ova, a neskôr security_onion.ova) a klikneme **Next**.
      iii. Appliance okno zobrazí odporúčané nastavenia v OVA archíve. Prijmeme predvolené nastavenia a klikneme na **Import** pre pokračovanie.



      iv. Keď je import proces ukončený, uvidíme nové virtuálne zariadenia pridané do inventáru VirtualBox-u v ľavom panely. Zariadenia sú teraz pripravené na použitie.
   c. Zapneme virtuálne zariadenia a prihlásime sa

i. Vyberieme a spustíme novo importované virtuálne zariadenia.
ii. Klikneme na tlačidlo **Štart** so zelenou šípkou v hornej časti okna aplikácie VirtualBox.
iii. Upozornenie: Ak získate nasledujúce dialógove okno:



- kliknite na položku **Change Network Settings** a nastavte svoj Bridged Adapter. Kliknite na rozbaľovaciu ponuku v zozname vedľa položky Name a vyberte sieťový adaptér (v každom počítači sa bude líšiť).
  Ak vaša sieť nie je nakonfigurovaná so službami DHCP, kliknite na položku **Change Network Settings** a vyberte NAT v rozbaľovacom poli Attached to.
  Nastavenia siete sú dostupné aj cez **Settings** vo VirtualBox-e alebo v ponuke virtuálneho zariadenia vyberte **Devices** > **Network** > **Network Settings**.
  Možno budete musieť vypnúť a zapnúť sieťový adaptér, aby sa zmena prejavila.

iv. Klikneme na tlačidlo OK. Zobrazí sa nové okno a spustí sa proces zavádzania virtuálneho zariadenia.
v. Po dokončení procesu zavádzania virtuálneho zariadenia, budeme požiadaný o používateľské meno a heslo. Zvolíme meno a heslo podľa uvedenej tabuľky vyššie (Používatelia).
   - Upozornenie: Všimnite si zameranie klávesnice a myši. Keď kliknete do okna virtuálneho zariadenia, myš a klávesnica bude ovládať hosťujúci operačný systém. Váš hostiteľský operačný systém už nebude detekovať stlačenie klávesov alebo pohyby myši. Stlačením pravého klávesu CTRL vrátite zameranie klávesnice a myši na hostiteľský operačný systém.

Kali Linux a Metasploitable

1. Stiahnutie a Inštalácia Metaspoitable 2 (cca 5 min)
   a. Postupujeme podľa návodu: https://beautyandthegeek.online/how-to-download-and-install-metasploitable-in-virtual-box/
2. Stiahnutie a Inštalácia Kali
   a. Stiahneme si Kali Linux image: https://www.kali.org/get-kali/#kali-bare-metal
      i. Poznámka: Vyberieme 64-bit verziu a „Installer“
   b. Stiahneme si Kali Linux virtual machine: https://www.kali.org/get-kali/#kali-virtual-machines
      i. Poznámka: Vyberieme 64-bit verziu a „VirtualBox“
         1. Prednastavené prihlasovacie údaje pre Kali virtual machine: kali/kali (používateľské meno/heslo)

c. Inštaláciu na Virtual Box robíme podľa postupu: https://www.kali.org/docs/virtualization/install-virtualbox-guest-vm/
   i. Poznámka: Kali Linux / Settings / System / Processor / Extended Features - Enable PAE/NX: Povolíme kvôli bezpečnostný dôvodom, viac info na https://en.wikipedia.org/wiki/NX_bit

Konfigurovanie Siete pre VM vo VirtualBox-e

1. Pre všetky virtuálne zariadenia je potrebné nastaviť tú istú sieť
   a. Vytvoríme NatNetwork
      i. Vo VirtualBox-e zvolíme „Tools“->“Preferences“->“Network“
      ii. Pridáme NatNetwork a dva krát klikneme na ňu pre úpravu.
      iii. Zvolíme názov siete alebo ho necháme predvolený a tak isto môžeme zmeniť Network CIDR.
   b. Pridáme novo vytvorenú NatNetwork sieť všetkým virtuálnym zariadeniam
      i. Klikneme na virtuálne zariadenia ľavým tlačidlom myši a zvolíme „Settings“->“Network“.
      ii. V poli „Attached to“ zvolíme NatNetwork a následne v poli „Name“ vyberieme názov, ktorý sme danej sieti dali a klikneme na „OK“.

Postup pre všetky varianty A, B, C:

Práca so zariadeniami

Zariadenie CyberOps Workstation predstavuje pre prácu KB analytika monitorovací a analytický nástroj. Toto zariadenie má operačný systém Linux a mnoho nástrojov, ktoré môže analytik využiť pri jeho práci. Niekoľko z nich si teraz ukážeme.

1. **Otvoríme zariadenie CyberOps Workstation**
   a. Vyskúšajte, či viete splniť nasledujúce úlohy
      i. Zobraziť pracovnú plochu
         - Aké položky sa nachádzajú na pracovnej ploche ?
      ii. Otvoriť terminál
         - Zobrazte procesy na vašom zariadení
      iii. Otvoriť webový prehliadač
         - Môžete sa dostať na stránku www.google.sk ?
      iv. Otvorte CyberOps Menu
         - Aké aplikácie sa v ňom nachádzajú ?
2. **Lokalizácia konfiguračných súborov:**
   a. Konfiguračné súbory sú uložené v priečinku /etc
   b. Zmena konfigurácie používateľom-špecifikovaného správania sa terminálu a jeho prispôsobenie
      i. Tieto nastavenie sa nachádzajú v priečinku bash.bashrc
         - Použi príkaz *$cat bash.bashrc* na zobrazenie priečinku
         - Zisti za pomoci internetu, čo sa nachádza v tomto priečinku a skús zmeniť nejaké nastavenie terminálu
   c. Konfiguračné súbory nie sú editovateľné pre normálneho používateľa

i. Musíme sa prihlásiť ako root pre ich editáciu
ii. Vypíš súbory v priečinku /etc
- Príkaz *$ls /etc*
- Skús upraviť nejaké súbory z ostatných zariadení
- Funguje editácia súborov ?

3. Overíme ostatné zariadenia

a. Zvoľte rovnaký postup pre ostatné zariadenia
i. Aké nástroje môžeme nájsť na ostatných zariadeniach ?
ii. Aké konfiguračné súbory nájdeme na týchto zariadeniach ?

4. Bonus: Úprava konfiguračných súborov pre služby

a. Konfiguračné súbory pre celý systém sa veľmi nelíšia od súborov používateľských aplikácií. nginx je ľahký webový server, ktorý je nainštalovaný vo virtuálnom počítači Cisco CyberOPS Workstation. nginx je možné prispôsobiť zmenou jeho konfiguračného súboru, ktorý sa nachádza v /etc/nginx.

b. Najprv otvoríme konfiguračný súbor nginx cez nano. Tu je použitý názov konfiguračného súboru custom_server.conf.
i. Všimneme si nižšie, že príkazu predchádza príkaz sudo. Po napísaní nano obsahuje medzeru a prepínač -l na zapnutie číslovania riadkov.
- Zadajte príkaz: *$ sudo nano -l /etc/nginx/custom_server.conf.* Na navigáciu v súbore použite klávesy so šípkami

ii. Zatiaľ čo konfiguračný súbor má veľa parametrov, nakonfigurujeme iba dva: port, na ktorom nginx počúva prichádzajúce pripojenia a adresár, z ktorého bude podávať webové stránky, vrátane indexového HTML súboru domovskej stránky.
- Na riadku 39 zmeňte číslo portu z 81 na 8080. Toto povie nginxu, aby počúval požiadavky HTTP na porte TCP 8080.
- Ďalej prejdite na riadok 47 a zmeňte cestu z /usr/share/nginx/html/ na /usr/share/nginx/html/text_ed_lab/
- Stlačte CTRL+X na uloženie súboru. Stlačte Y a potom ENTER na potvrdenie a použitie custom_server.conf ako názov súboru.
- Zadajte príkaz na spustenie nginx pomocou upraveného konfiguračného súboru: *$ sudo nginx -c custom_server.conf*
- Kliknite na ikonu webového prehliadača na spodnom panely pre spustenie Firefoxu.
- Do panela s adresou zadaj 127.0.0.1:8080, pre pripojenie ku webovému serveru hosťovanému na lokálnom počítači na porte 8080. Mala by sa zobraziť stránka súvisiaca s týmto laboratóriom.
  - Po úspešnom otvorení domovskej stránky nginx sa pozrite na správu o pripojení v okne terminálu. Na čo odkazuje chybové hlásenie?

iii. Pre vypnutie webového serveru nginx, stlač kláves ENTER, aby si dostal príkazový riadok a zadajte nasledovný príkaz v okne terminálu:
- *$ sudo pkill nginx*
- Otestujte, či je server nginx skutočne vypnutý, najprv vymazaním nedávnej histórie na webovom prehliadači, potom zatvorte a znova otvorte webový prehliadač a prejdi na domovskú stránku nginx na 127.0.0.1:8080. Zobrazí sa webová stránka?

Linux služby

Nasledujúce kroky vykonajte na všetkých zariadeniach.

1. **Zobrazte služby, ktoré aktuálne bežia**
    a. Zadajte príkaz *$sudo ps -elf* na zobrazenie všetkých procesov, ktoré bežia na pozadí
        i. Prečo sme použili príkaz ako root?
    b. Zadajte príkaz na zobrazenie procesnej hierarchie
        i. Zapnite nejaký proces na zariadení, ak nebeží, ktorý chcete zobraziť
            1. Príkaz *$sudo „Cesta k procesu"*
        ii. Príkaz *$ sudo ps -ejH*
            1. Popíšte výpis v terminály
2. **Služby serverov**
    a. Servery sú v podstate programy, ktoré sa často spúšťajú pri bootovaný systému
    b. Úloha vykonávaná serverom je služba(service)
        i. Netstat príkaz je vynikajúci nástroj na zobrazenie serverových služieb v sieti
        ii. V terminály zadajte príkaz *$netstat*
            1. Aké údaje môžeme vyčítať z výpisu?
        iii. Vyskúšajte príkaz s prepínačmi *$ netstat -tunap*
            1. Aké údaje vidíme teraz?
            2. Zistite čo znamenajú prepínače -tunap
                a. Použite príkaz *$ man netstat*
    c. Niekedy je dobré spojiť príkaz ps s netstat
        i. Zistite z výpisu ps aké ma PID nginx
        ii. Zadajte príkaz *$ sudo ps -elf | grep [proces PID]*
            1. Popíšte údaje, ktoré sú zobrazené vo výpise

3. **Použi telnet na testovanie TCP služieb**
    a. telnet je nezabezpečená shell aplikácia na vzdialené manažovanie sieťových zariadení
    b. namiesto telnet-u sa používa ssh, ale telnet je dobrý na rýchle testovanie a zbieranie informácii o TCP služieb
        i. Overíme, že proces, ktorý práve beží na porte TCP 80(alebo 8080) je naozaj webový server a nie malware od útočníka pod rovnakým názvom
        ii. Zadáme príkaz $ telnet 127.0.0.18080 alebo len port 80
            1. Keď nás pripojí na server zadáme len náhodný reťazec písmen
            2. Nginx nerozumie reťazcu písmen, preto nám pošle chybu vo forme web stránky
                a. Aké informácie o nginx sa môžeme dozvedieť z tejto chyby?
4. **Overíme služby aj na iných zariadeniach**
    a. Spustíme postupne zariadenia a postupujeme podľa krokov vyššie
        i. Namiesto služby nginx zvolíme inú, ktorá momentálne beží na danom zariadení (ak beží)
            1. Aké služby bežia na zariadeniach?
            2. Aké služby serverov bežia na zariadeniach?

Tabuľka s príkazmi pre Linux

Príkaz	Prepínače	Akcia
ifconfig <interface> <ip address> netmask <ip mask> up		*Priradenie ip adresy zariadeniu v Linuxe*
route add default gw <ip_address> <interface>		*Priradenie default gateway*
ping <ip address>		*Overenie spojenia k danej adrese*
ip addr show		*Zobrazí priradené ip adresy*
Ping <IP address>	HTTPS://VITUX.COM/LINUX-PING-COMMAND/#POST-675	*Posielanie ICMP paketov na danú adresu*

Záver

- V závislosti od služby môže byť k dispozícii viac možností konfigurácie.
- Umiestnenie konfiguračného súboru, syntax a dostupné parametre sa budú líšiť od služby k službe.
- Práva sú veľmi častou príčinou problémov. Uistite sa, že máte správne práva predtým ako upravíte konfiguračné súbory.
- Skôr než sa zmeny prejavia, služby musia byť častejšie reštartované.

Otázky

- Aké sú výhody používania netstat?
- Aké sú nevýhody používania Telnetu? Je to bezpečné?